

POLITICO PRO

U.S. surveillance industry fears crippling effect of Chinese tech ban

By Shawna Chen

08/08/2019 02:47 PM EDT

The U.S. video surveillance industry, largely powered by Chinese technology, says it's being unfairly targeted as part of the Trump administration's push to block Huawei, ZTE and other firms with close ties to Beijing from American networks.

The thousands of companies that make up the surveillance marketplace, and sell much of their equipment to federal agencies for use in locations like military bases and courthouses, face major financial losses as the White House begins to ban Chinese telecommunications and video surveillance components it says threaten U.S. national security.

On Wednesday, the Office of Management and Budget released an [interim rule](#) barring federal agencies from buying equipment from five companies — Huawei, ZTE, Dahua Technology, Hytera Communications and Hikvision Digital Technology — in a procedural step to implement a provision in the 2019 National Defense Authorization Act. The ban takes effect next week.

The administration is expected to put in place additional — and even more far-reaching — restrictions next year that would forbid any U.S. contractor from using equipment from the five companies. Lawmakers and Trump administration officials worry that the widespread use of cheap Chinese components could allow Beijing to build a vast surveillance network in the U.S.

But many in the industry said they were blindsided to find Dahua and Hikvision, two of the world's largest suppliers of video components, lumped in with the Chinese telecommunications giants Huawei and ZTE, which have both been the subject of much U.S. scrutiny due to concerns about 5G security.

Dahua and Hikvision have an estimated 40 percent market share in global video equipment sales, according to Memoori, a business intelligence service. The companies' components are used by cities around the world to monitor streets and schools as well as used in banks, office buildings and hospitals as part of video surveillance systems.

Additionally, about 20 percent of surveillance equipment used by small- and medium-sized U.S. businesses is manufactured by Hikvision and Dahua, according to Jake Parker, senior director of government relations at the Security Industry Association, which represents about 1,000 U.S. video surveillance companies as well as Dahua and Hikvision.

DISSEMINATED BY MERCURY PUBLIC AFFAIRS, A REGISTERED FOREIGN AGENT, ON BEHALF OF HIKVISION USA. MORE INFORMATION IS ON FILE WITH THE DEPARTMENT OF JUSTICE, WASHINGTON, DC.

The U.S. government has pointed to the fact that the Chinese government owns 40 percent of Hikvision and that an independent researcher discovered backdoors in Dahua cameras and recorders in 2017 to support the companies' inclusion in the ban. Hikvision and Dahua are both based in Hangzhou, China.

But industry executives and representatives say the nature of most video surveillance systems makes it difficult, if not impossible, to manipulate in a way that would allow the Chinese government to spy on U.S. facilities. What's more, they say, most of the equipment operates on a closed-circuit network and does not connect to the internet.

"It's worthy of concern but a fanciful idea," said a person familiar with Hikvision who asked not to be named because the person is not authorized to speak to the press.

Hikvision told POLITICO in a statement that it is "gravely disappointed that the 2019 NDAA provision will take effect without a review or investigation to warrant the video surveillance technology restrictions."

They added that the company "strictly complies" with laws and regulations and supports a standards-based approach to federal prohibitions instead of one based on national origin.

Peter Micek, general counsel at digital rights group Access Now, agrees that the U.S. should be looking at the video surveillance industry across the board and not just singling out companies from specific countries.

"Politically motivated restrictions like this one don't provide the comprehensive, human rights-based frameworks that we need and deserve," he said in an email, adding that the government should set security standards or assessments for all companies that provide the government with surveillance equipment.

What is most concerning now for video surveillance companies, especially smaller ones, is that the federal ban could spread to states or cause the corporate sector to take similar action.

Carl Shumate of The Alarm Company, based in Florida, said the "crazy" trickle-down effect of the ban could result in tens of millions of dollars in losses. It could cost the company as much as \$50 million to simply remove Chinese equipment from nearly 40 correction facilities and replace it with non-Hikvision components, he said. The Florida Department of Juvenile Justice is already considering removing Chinese equipment from its facilities.

Greg Nuckles, chief financial officer of Tennessee audio and video surveillance company SkyCop, called the ban a form of "blacklisting" that could lead to public safety problems if, for instance, his company has to replace equipment at sensitive locations, potentially leaving them without security for weeks.

Beyond general concerns about Chinese technology, the federal government hasn't provided an explanation of the specific national security concerns related to Dahua or Hikvision, said Parker, the industry spokesperson.

The Federal Acquisition Regulatory Council is developing specifics for exactly which parts and components will be included in the ban.

Jacob Wood, spokesperson for the Office of Management and Budget, said that "the administration has a strong commitment to defending our nation from foreign adversaries, and will fully comply with Congress on the implementation of the prohibition of Chinese telecom and video surveillance equipment companies, including Huawei."

Rep. [Vicky Hartzler](#) (R-Mo.), senior member of the House Armed Services Committee who originally introduced the amendment to add Hikvision and Dahua to the provision, said in a press release last May that "we must face the reality that the Chinese government is using every avenue at its disposal to target the United States, including expanding the role of Chinese companies in the U.S. domestic communications and public safety sectors."

Her amendment, she said, would prevent China from creating a "video surveillance network within federal agencies."